

# Assurance Cases Overview

---

Howard Lipson, CERT [vita<sup>1</sup>]

Copyright © 2007-2008 Carnegie Mellon University

2007-1-4; Updated 2008-5-23

L1 / (E), L, M<sup>2</sup>

Our objective for the Assurance Cases (AC) content area of the Build Security In (BSI) Web site is to raise awareness about emerging methods and tools for assuring security properties of systems. In this content area, we introduce the concepts and benefits of developing and maintaining assurance cases for security. In particular, we describe the benefits of integrating assurance cases for security into the software development life cycle (SDLC) by “building assurance in” from the outset.

Elsewhere on the BSI Web site, the reader can learn about best practices, tools, and techniques that can help developers build security into their software. But the mere existence or claimed use of one or more of these best practices, tools, or techniques does not constitute an adequate assurance case. For example, in support of an overarching security claim (e.g., that a system is acceptably secure), security assurance cases must provide evidence that particular best practices, tools, and techniques were properly applied and must indicate by whom they were applied and their extent of coverage. Moreover, unlike many product certifications that quickly grow stale because they are merely snapshots in time of an infrequently applied certification process, a security assurance case should provide evidence that the practices, tools, or techniques being used to improve security were actually applied to the currently released version of the software (or that the results were invariant to any of the code changes that subsequently occurred).

A security assurance case uses a structured set of arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security properties. The case should be amenable to review by a wide variety of stakeholders. Although tool support is available, the creation and documentation of a security case can be a demanding and time-consuming process. Yet, similarities may exist among different security cases in the structure and other characteristics of the claims, arguments, and evidence used to construct the cases. A catalog of patterns (i.e., templates) for security assurance cases can facilitate the process of creating and documenting an individual case. Moreover, assurance case patterns offer the benefits of reuse and repeatability of process, as well as providing some notion of coverage or completeness of the evidence.

## Articles in this Content Area

The first article in this content area provides an introduction to the fundamentals of security assurance cases. We’ve added a second article to this content area (new for 2008) that provides more detail on the nature of evidence that can contribute to building a credible security assurance case. We expect that more documents will be added over time and that the existing material will continue to evolve. The current documents in this content area are described below.

- **Arguing Security – Creating Security Assurance Cases<sup>3</sup>**  
This introductory document describes the basic concepts associated with assurance cases and how they can be applied in the security domain (where they are known as *security cases*). What are security cases? What do security cases look like (i.e., what is their structure)? Why are they useful? When developing security cases it is common for arguments with the same structure to appear in many different contexts. A *security case pattern* takes advantage of this structural similarity and can reduce the effort needed to develop a security case. We explore an example of a security case, and a security case pattern, expressed graphically in Goal Structuring Notation.
- **Evidence of Assurance: Laying the Foundation for a Credible Security Case<sup>4</sup> (New)**  
A security case bears considerable resemblance to a legal case, and demonstrates that security claims about a given system are valid. Persuasive argumentation plays a major role, but the credibility of

---

1. [http://buildsecurityin.us-cert.gov/bsi/about\\_us/authors/15-BSI.html](http://buildsecurityin.us-cert.gov/bsi/about_us/authors/15-BSI.html) (Lipson, Howard F.)

the arguments and of the security case itself ultimately rests on a foundation of evidence. This article describes and gives examples of several of the *kinds* of evidence that can contribute to a security case. Our main focus is on how to understand, gather, and generate the kinds of evidence that can build a strong foundation for a credible security case.

## Future Plans

Our future plans for the Assurance Cases content area (assuming the availability of resources) include steadily moving the focus of the material from introductory articles in the knowledge category toward material that can help establish security assurance cases as a best practice. Upcoming articles will provide detailed guidance on the practical steps that managers and practitioners can take to analyze and improve each phase of their software development life cycle process by applying security assurance case tools and techniques. Tutorial-level material will provide guidance on specific aspects of constructing a security case, such as how to generate, gather, evaluate, organize, and combine items of evidence to improve the overall evidentiary strength of your case. The use of security cases to support governance and management will be further elaborated. Our goal will be to help the reader learn how to use security assurance cases as a best practice to progress from ad hoc approaches, such as the use of unstructured security checklists, to the development and use of structured, reviewable arguments, backed by evidence that can be gathered continually throughout the SDLC (including system operations) and that can serve as a basis for continuous security improvement. As always, feedback and technical contributions from the community are most welcome.

## Carnegie Mellon Copyright

---

Copyright © Carnegie Mellon University 2005-2010.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu)<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

### NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

---

1. <mailto:permission@sei.cmu.edu>